

Algebraic characterisation of one-way patterns

Vedran Dunjko

Department of Physics, Heriot-Watt University, UK
School of Informatics, University of Edinburgh, UK

Elham Kashefi

School of Informatics, University of Edinburgh, UK

We give a complete structural characterisation of the map the positive branch of a one-way pattern implements. We start with the representation of the positive branch in terms of the phase map decomposition [4], which is then further analysed to obtain the primary structure of the matrix M , representing the phase map decomposition in the computational basis. Using this approach we obtain some preliminary results on the connection between the columns structure of a given unitary and the angles of measurements in a pattern that implements it. We believe this work is a step forward towards a full characterisation of those unitaries with an efficient one-way model implementation.

1 Introduction

The one-way model of quantum computation has drawn considerable attention, mainly because it suggests different physical realisations of quantum computing [6, 7]. In this model quantum states are transformed using single qubit measurements on an entangled state (called *open graph state*), which is prepared from an input state by performing controlled-Z operations on pairs of qubits, including the input system and auxiliary qubits prepared in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ state. Quantum measurements are probabilistic in general, and can drive the computation over 2^n different branches, where n is the number of measurements. However, there exist sufficient conditions based on the structure of the graph state where the computation can be controlled by means of single qubit corrections, dependent on the previous measurement outcomes, so that the entire computation becomes deterministic [6, 3, 2, 7]. In such a deterministic computation, all the branches implement the same unitary map introduced by the *positive branch* (also known as the post-selected branch) which corresponds to the scenario in which every measurement collapses the qubit states to pre-selected states, typically $|+\alpha_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha_i}|1\rangle)$.

We give a complete structural characterisation of the map the positive branch of a one-way pattern implements. The positive branch of a one-way pattern can be expressed in terms of a *phase map decomposition* $R\Phi P$ [4, 1], which we then further analyse to obtain the primary structure of the matrix M which represents $R\Phi P$ in the computational basis. The columns of M can be written as:

$$M\mathbf{e}_i = \varepsilon_i B_i \vec{\phi}$$

where ε_i are complex scalars of norm one, parametrized by the measurement angles of the input qubits, B_i are signs matrices, depending on the geometry of underlying open graph state, and $\vec{\phi}$ is a vector parametrized by the measurement angles of measured auxiliary qubits. The primary structure offers the following simple observations concerning the matrix M :

- The first column is determined only by the geometry of the open graph state and the measurement angles of the auxiliary qubits.
- All the entries of each column are sums of complex numbers of a fixed set, possibly differing in signs.

- The measurement angles of input qubits parametrize the global phase factors of columns of matrix M , which otherwise depend only on the geometry of the open graph state and the measurement angles of the auxiliary qubits.

Moreover we can use this characterisation to easily prove the following simple lemma about uniform determinism. Recall that a pattern is called uniform deterministic if it is deterministic for all possible angles of measurements.

Lemma 1 *A pattern is uniformly deterministic if and only if it is deterministic for all possible choices of auxiliary measurement angles.*

We then proceed to meticulously dissect the B_i matrices to reveal their structure given by the following decomposition:

$$B_i = \gamma_i \Delta_i S B N \Omega_i,$$

where γ_i is a sign, which depends on the adjacency of the input qubits, Δ_i, S, N and Ω_i are diagonal sign matrices parameterised by the adjacencies of the set of input to the set of output qubits, the adjacency of output qubits, the adjacency of measured auxiliary qubits, and the adjacency of the set of input to the set of measured auxiliary qubits, respectively. B is a full sign matrix, parametrized by the adjacency between the set of output and the set of measured auxiliary qubits. The scalars and the matrices are given in terms of explicit functions on graphs, represented purely graph-theoretically, as adjacency matrices, and as lists of edges. These functions have group-theoretical properties, which we feel could further be utilised to help elucidate the following open problems:

- Simulation of given unitaries directly in the one-way model, *i.e.* without reference to the circuit-based model.
- Characterisation of graph states which implement the same map in the positive branch.
- A refined characterisation of determinism.
- Characterisation of the pointless measurement [5] which is a key element in defining new error correcting codes.

2 Preliminaries

In this section we briefly review the one-way model, and present the Phase Map Decomposition [4, 1] of one-way patterns. A brief summary of linear algebra, and the notation used throughout this paper is given in the Appendix.

The process of computation in the one-way model can be summarised in the following steps:

1. The setting up of n input qubits in an input state $|\psi\rangle$
2. The addition of $m - n$ auxiliary qubits, prepared in the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
3. The pairwise entanglement of some qubits by means of the $\wedge Z$ interaction. This interaction is represented by an open graph state, an ordered triplet (Γ, I, O) , where Γ represents the entanglement graph (two qubits are entangled if and only if the corresponding vertices are adjacent), I is the set of input qubits/vertices and O is the set of output qubits/vertices which is a subset of the auxiliary qubits.
4. The measurement of the input qubits and non-output auxiliary qubits (which we call *pure auxiliary qubits*) in the (X, Y) Bloch sphere plane, that is in the basis pairs $\{|+\alpha_i\rangle, |-\alpha_i\rangle\}$, parametrized by a set of measurement angles $\{\alpha_1, \dots, \alpha_{m-n}\}$. Here we use the following shorthand notation: $|\pm\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle)$. The set O corresponds to the qubits which will not be measured.

Without loss of generality we assume input and output qubits are not overlapping. This is not a restriction, as additional auxiliary qubits can be added, which will correspond to the overlapping qubits, to which the quantum state of the overlapping qubits can be teleported. It can be easily shown these two scenarios are equivalent. As quantum measurements are generally probabilistic, the pattern implements a general completely positive map [8]. The scenario in which each measurement corresponds to the projection into the state $|+\alpha_i\rangle$ state is called the positive branch, and the positive branch realises a linear transformation of the Hilbert space of the input qubits to the Hilbert space of the output qubits. The corresponding model is called projection-based quantum computing.

We focus on the positive branch only, for this not to be a restriction, it will suffice that the graph Γ , defined by the underlying graph state, fulfils the graph-theoretical condition of having *flow* or *generalised flow* [3, 2], as then by means of local single qubit corrections, conditioned on sequential measurement outcomes, the entire quantum evolution of the system can be driven to be equal to the positive branch.

We will choose the labelling of qubits so that the first n labels correspond to the input qubits, the following $a = m - 2n$ correspond to the measured auxiliary qubits (which we will call pure auxiliaries), and the last n correspond to the output qubits. We have assumed that in a given one-way pattern all the input qubits are measured first (the first round of the computation). One could easily adapt the whole discussion of this paper to the scenario where there exist no input qubits or some of the pure auxiliary qubits are also measured in the first round by labelling such qubits among the first n labels.

The measuring of a qubit in the $\{|\pm_\alpha\rangle\}$ basis is equivalent to first locally rotating that same qubit by the local Z_α unitary transformation, followed by a measurement in the $\{|\pm\rangle\}$ basis. For reference reasons, here we give the matrix representations of $\wedge Z$ and Z_α in the computational basis:

$$\wedge Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad Z_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$$

Hence, since $\wedge Z$ and Z_α are commuting, the projection-based computation process can be restated as follows:

1. The setting up of n input qubits in the input state $|\psi\rangle$
2. The addition of $m - n$ auxiliary qubits, set in the state $|+\rangle$
3. The application of local Z rotations to the input and $m - 2n$ auxiliary qubits, corresponding to the measurement angles $\{\alpha_1, \dots, \alpha_{m-n}\}$
4. The pairwise entanglement of some qubits by means of the $\wedge Z$ interaction. This interaction is represented by an open graph state, an ordered triplet (Γ, I, O) , where Γ represents the entanglement graph (two qubits are entangled if and only if the corresponding vertices are adjacent), I is the set of input qubits/vertices and O is an n qubit/vertex subset of the auxiliary qubits representing the output qubits
5. The projection of the input qubits and $m - 2n$ auxiliary qubits to the $|+\rangle$ state

The first and second steps above comprise an embedding of a 2^n dimensional Hilbert space to a 2^m dimensional Hilbert space which we will denote P (for *preparation map*), given explicitly as:

$$P : |\psi\rangle \rightarrow |\psi\rangle \otimes |+\rangle^{\otimes(m-n)}$$

The application of the $m - n$ local rotations implements a map which we denote Φ_1 :

$$\Phi_1 = \prod_{i=1}^{m-n} \mathbf{Z}_{-\alpha_i}^{(i)}$$

$\mathbf{Z}_{-\alpha_i}^{(i)}$ denotes an m -qubit unitary, which acts trivially on the composite subspaces of all qubits, except for the i^{th} qubit, where it performs the $\mathbf{Z}_{-\alpha_i}$ rotation. Note that this is an operator on a 2^m dimensional Hilbert space. We collect the entangling interactions, $\wedge \mathbf{Z}$, into the map Φ_2 :

$$\Phi_2 = \prod_{(i,j) \in \mathcal{E}} \wedge \mathbf{Z}_{i,j}$$

where the indexing goes across the set of unordered edges \mathcal{E} of the graph state given by the graph Γ :

$$\mathcal{E} = \{ \{v_i, v_j\} \mid \{v_i, v_j\} \subseteq V(\Gamma) \}$$

The operator $\wedge \mathbf{Z}_{i,j}$ is an m -qubit unitary transformation, which acts trivially on the component subspaces of all qubits, except the composite subspace of qubits i and j , where it performs the $\wedge \mathbf{Z}$ transformation. We call the cumulative action of the latter two maps the *Phase map* and denote it Φ :

$$\Phi = \Phi_2 \Phi_1$$

The last step of the computation consists of projecting the first $m - n$ qubits to the state $|+\rangle$, which we denote R (for *restriction map*):

$$R = \langle + |^{\otimes (m-n)} \otimes I_{2^n}$$

where I_{2^n} is the identity map on the 2^n -dimensional Hilbert space.

Now, the entire process of computation in the projection-based model is represented by

$$R\Phi P$$

and we call this representation the *Phase map decomposition* of a given unitary operator implemented in the one-way pattern [4, 1]. Note that one can also derive directly a phase map decomposition for any unitary operators without any references to the one-way pattern [4].

3 Structural characterisation of the Phase map decomposition

Let $\{|i\rangle\}_{i=1}^{2^n}$ denote the standard computational orthonormal basis of a 2^n dimensional complex Hilbert space. Every computational basis in this representation describes a sequence of 0-1 which is the binary representation of the integer value $i - 1$. Therefore $i - 1$ represented in binary, encodes the choice of states $|0\rangle$ or $|1\rangle$ in the component single qubit state spaces. For example, the state $|3\rangle$, in a four qubit setting, represents the state $|0\rangle|0\rangle|1\rangle|0\rangle$ as $(3 - 1) = (0010)_2$.

Next we refine the expression $R\Phi P|i\rangle$ to obtain the structure of the i^{th} column of the matrix which represents $R\Phi P$ in the computational basis.

Theorem 1 *Let $R\Phi P$ be a phase map decomposition corresponding to a positive branch of a one-way pattern over m qubits, with n non-overlapping input and output qubits, $a = m - 2n$ measured auxiliary qubits, with the set of measurement angles $\{-\alpha_1, \dots, -\alpha_{n+a}\}$. Then, the matrix M representing $R\Phi P$ is characterised with respect to columns by the following equality:*

$$M\mathbf{e}_i = \varepsilon_i B_i \vec{\phi} \quad (1)$$

where

- \mathbf{e}_i is the i^{th} vector of the canonical basis
- $\varepsilon_i = \left(\bigotimes_{k=1}^n \begin{bmatrix} 1 \\ e^{i\alpha_k} \end{bmatrix}, \mathbf{e}_i \right)$, with (\cdot, \cdot) denoting the symmetric dot product
- $\vec{\phi} = \bigotimes_{k=n+1}^{n+a} \begin{bmatrix} 1 \\ e^{i\alpha_k} \end{bmatrix}$
- B_i is a matrix of signs of dimension $2^n \times 2^a$, which depends on the underlying graph state, and we call them the sign pattern matrices

Proof. The proof is based on simple linear algebra manipulations so we put the details in the Appendix. The main properties used are the diagonal form of both Z_α and $\wedge Z$ in the computational basis. The complex phases arising from the Z_α local rotations are collected in the $\vec{\phi}$ vector and in the scalars ε_i , and the diagonal of the Φ_2 entangling operation gets spread across the sign pattern matrices B_i . The proof itself presents this structure of the B_i matrices (see Appendix)

$$B_i = \sum_{j=1}^{2^n} \sum_{l=1}^{2^{(m-2n)}} b_{[(i-1)2^{(m-n)} + (l-1)2^n + j]} |j\rangle\langle l| \quad (2)$$

These properties will be used in the following section. \square

For simplicity, in the expression for $\vec{\phi}$ as a numerical vector, we omit a normalising factor of $2^{-(\frac{m-2n}{2})}$, along with the scaling factor $(2^{-(m-n)})$ of the B_i matrices as it has no bearing on the structure we wish to present.

A few direct consequences of Theorem 1 are easily checked:

- The first column of M is parametrized by the measurement angles of pure auxiliary qubits only, as $\varepsilon_1 = 1$.
- For every column i , the entries per row, are of the form

$$\varepsilon_i(r, \vec{\phi}) \quad (3)$$

for some vector of signs r . So, entries of a column are sums of the same set of elements, varying possibly in signs only.

- From 3 it is clear that every entry of every column is a sum of elements of the set of entries of the vector $\vec{\phi}$ varying in signs, multiplied by the column's corresponding global phase factor ε_i .

As mentioned before we can also prove the following simple lemma about the uniform determinism.

Lemma 2 *A pattern is uniformly deterministic if and only if it is deterministic for all possible choices of auxiliary measurement angles.*

Proof. Due to Theorem 1, the measurement angles of the input qubits appear only as global phase factors of the columns of M , and these global factors ε_i are of norm one. Hence the choice of measurement angles of input qubits do not influence the norm of the columns. Also regardless of the measurement angles of the input qubits (as the product of two complex numbers of norm 1 is always norm 1), the matrix M is orthogonal since its columns are orthonormal. Therefore, uniform determinism can only depend on the measurement angles of the measured auxiliary qubits. \square

The statement of Theorem 1 indicates a direct method for addressing problems of equalities of patterns, and of simulating a given unitary evolution of a quantum system in the one-way model. For the first problem, we have to evaluate and check the equalities of two expressions of the form of the right-hand side of 1. However, that entails knowing how to construct the sign pattern matrices from given graph states. This demands further analysis of the sign pattern matrices, which will be the topic of the next two sections.

4 Graph-theoretical characterisation of sign pattern matrices

In the proof of the Theorem 1, the matrices B_i were defined as representations of the expression

$$\sum_{j=1}^{2^n} \sum_{l=1}^{2^{(m-2n)}} b_{[(i-1)2^{(m-n)}+(l-1)2^n+j]} |j\rangle \langle l|$$

in the computational basis, and in that representation b_l corresponds to the l^{th} diagonal entry of the matrix representation of Φ_2 in that same basis. We now link the graph theoretical aspects of the graph state defining the pattern and the above expression.

Recall that the $\wedge Z$ interaction is diagonal in the computational basis, hence the map Φ_2 is diagonal in that basis as well. We introduce the *sign parity* function SP defined as

$$SP(k) = (-1)^k$$

as it visually simplifies the expressions. It was shown in [4] that b_l , the l^{th} diagonal element of Φ_2 is given by the following expression:

$$b_l = SP \left(\sum_{(i,j) \in \mathcal{E}} x_i x_j \right),$$

where x_k was defined as the k^{th} most significant digit (k^{th} digit from the left, including leading zeroes) of $l-1$ represented in binary, and \mathcal{E} is an unordered list of edges of the entanglement graph state, represented by the graph Γ . It is easy to give a graph-theoretical representation for the expression for b_l . It can be shown that the expression $\sum_{(i,j) \in \mathcal{E}} x_i x_j$, where x_i and x_j are functions of l , counts the number of edges of a vertex-induced subgraph of the graph Γ , where the vertex set which induces the subgraph is determined by l . In order to explain how l determines a subset of vertices, we define a function which realises this vertex determination process by an integer:

Definition 3 *If V is a set of vertices, labelled with integers $\{1, \dots, m\}$, and k is an integer in $\{1, \dots, 2^m\}$ then the selection function Sel is defined as follows: $Sel(V, k)$ is a subset of V such that for the vertex labelled with l (which we present in the subscript) $v_l \in V$, $v_l \in Sel(V, k)$ holds if and only if the l^{th} most significant digit of the m digit binary representation (including leading zeroes) of $k-1$ is 1.*

This function easily extends to any finite totally ordered set O , via an order-preserving bijection between O and $\{1, \dots, |O|\}$. Also, we will use the expression of the form *a subset of S , selected by (the integer) k* to mean precisely $Sel(S, k)$. Using the introduced terminology, b_l is the sign parity of the number of edges of the vertex-induced subgraph of Γ induced by a subset of the vertices of Γ , *selected by l* .

Now, we can direct our attention to the expression 2 and state the following proposition about the graph-theoretical characterisation of the sign pattern matrices B_i .

Proposition 4 *Let Γ be the a graph of a graph state, with vertices labelled by integers $\{1, \dots, m\}$, such that the first n and last n correspond to input and output vertices (qubits) respectively, and the remaining $a = m - 2n$ vertices correspond to the measured auxiliary (pure auxiliary) vertices (qubits) then every entry $(B_i)_{p,q}$, is a sign parity of the number of edges of a vertex-induced subgraph of Γ , and the inducing set of vertices V' depends on the triplet (i, p, q) as follows:*

$$V' = Sel(I, i) \cup Sel(Aux, q) \cup Sel(O, p),$$

where O denotes the subset of output vertices, Aux denotes the subset of pure auxiliary vertices, and I denotes the subset of input qubits.

Proof. From the graph-theoretical characterisation of the diagonal elements of Φ_2 the expression for $b'_{i,s}$ and the binary representation of the index of b in 2 it is easy to see that the Proposition holds. \square

Using the terminology of the selection function we can restate this proposition in the following fashion. The (p, q) entry of the sign pattern matrix B_i is the sign parity of the number of edges of a vertex induced subgraph of Γ . This inducing subset is a union of subsets of the input, output and pure auxiliary vertices. The index of B_i (the corresponding column of M) i selects a subset of the input vertices. The row p selects a subset of the output vertices. Finally, the column q selects a subset of the pure auxiliary vertices.

Theorem 1 and Proposition 4 could be potentially used in address the following problems. The equality of patterns and the simulation of a given unitary. In doing so, the essential expression we need to calculate is the expression 3. If we are interested in verifying the equality of two patterns, we need to calculate and compare the matrices of their phase map decompositions, given by the Theorem 1. This entails calculating the dot product of the rows of the matrices B_i and the vectors $\vec{\phi}$. Similarly, if we are trying to simulate a given unitary, expressions 3 which will contain variables, as we go across all entries of all columns of the matrix M , will form the left-hand sides of a system of equations we will have to solve (the right-hand side being the entries of the given unitary).

The dot product of rows of the sign pattern matrices and the vector $\vec{\phi}$ is in general hard to evaluate, as both vectors have an exponential lengths in the number of pure auxiliary qubits. However, the vector $\vec{\phi}$ is represented as a Kronecker product of vectors of length 2, as it corresponds to a state space vector which can be represented as a tensor product of the minimal, two-dimensional component spaces. Such a representation contains the same number of 2-dimensional vectors, as there are measured auxiliary qubits, and so is efficient. The ability to represent the rows of the sign pattern matrices in such a compact form might assist in deriving techniques for solving and evaluating such expressions efficiently.

Hence, in the following section we focus our attention to the structure of rows of the sign pattern matrices and present the decomposition theorem for the sign pattern matrices.

5 Decomposition of the sign pattern matrices

If we turn our attention to any row p of any matrix B_i , from Proposition 4 we can see that by selecting the index i (equivalently, a column of M) and a row p we have fixed a subset of the input qubits and a subset of output qubits, respectively. The p^{th} row of B_i is then generated by the sign parities of the numbers of edges of the vertex-induced subgraphs of Γ , where the inducing set is a union of the selected fixed sets of input and output vertices, and the entry of that row (the column of B_i) then selects the additional subset of the pure auxiliary vertices.

Therefore, for fixed p and i , the corresponding row of B_i , which we denote by r , is given entry-wise by the following expression:

$$(r)_k = SP \left(\#E \left(\Gamma_{Sel(I,i) \cup Sel(O,p) \cup Sel(Aux,k)} \right) \right) \quad (4)$$

where $\#E(\Gamma)$ denotes the number of edges of the graph Γ , and for a given graph Γ over the set of vertices V , and $V' \subseteq V$, $\Gamma_{V'}$ denotes a vertex-induced subgraph of the graph Γ induced by the set V' . In expression 4 only the subsets of pure auxiliary vertices change as we go across the entries of r .

The subgraph inducing vertex subset is expressed as a union of three subsets, two constant, and one variable. Let us denote $A = Sel(O, p)$, $B = Sel(I, i)$ and $X = Sel(Aux, k)$. As we will be dealing with only one graph at a time, we will drop the graph designation and use the shorthand $\#E(A)$ instead of $\#E(\Gamma_A)$. Also, with $\#E(Y \leftrightarrow Z)$ we denote the number of edges joining vertices in Y with vertices in Z in the graph we are observing. It is then easy to see that

$$\#E(A \cup X \cup B) = \#E(A) + \#E(X) + \#E(B) + \#E(B \leftrightarrow A) + \#E(A \leftrightarrow X) + \#E(B \leftrightarrow X) \quad (5)$$

Equality 5 and the fact that the sign parity function is a homomorphism from additive monoid of integers to the multiplicative monoid of integers ($SP(i + j) = SP(i)SP(j)$) will give a basis for the decomposition of the sign parity matrices. Therefore, we can express the vector r with respect to the entries as follows:

$$(r)_k = SP(\#E(B)) SP(\#E(B \leftrightarrow A)) SP(\#E(A)) SP(\#E(A \leftrightarrow X)) SP(\#E(X)) SP(\#E(B \leftrightarrow X)) \quad (6)$$

Note the dependencies of the factors of the right-hand side of 6 with respect to the explicit parameter k of r , parameter p which is the row selection of B_i and parameter i itself which is the choice of the column of $M B_i$.

1. $SP(\#E(B))$ depends on i only, as it corresponds to a choice of the subset of output vertices.
2. $SP(\#E(B \leftrightarrow A))$ depends on both i and p , but is independent of k .
3. $SP(\#E(A))$ depends on p only as it corresponds to a choice of input vertices.
4. $SP(\#E(A \leftrightarrow X))$ depends on p and k .
5. $SP(\#E(X))$ depends on k only.
6. $SP(\#E(B \leftrightarrow X))$ depends on i and k .

We have represented the fixed row of a sign pattern matrix r by its entries. We will now represent r by using vector functions, defined on graphs, as that will allow for a simple characterisation of B_i matrix entries.

First, we note that, in the list of dependencies of factors which make up an entry of f , the first three are constants in k . The last three factors depend on k , and we shall represent them as components of values (which are vectors) of two different vector functions on graphs attain.

We define a function on simple graphs whose set of vertices are equipped with a strict order.

Definition 5 Let Γ be a simple graph, where the set of vertices is equipped with a strict order. We define $\mathcal{P}(\Gamma)$ to be a vector of signs of length $2^{|V|}$ given by the following components

$$(\mathcal{P}(\Gamma))_k = SP(\#E(\text{Sel}(V, k)))$$

for all $k = 1, \dots, 2^{|V|}$.

Since we will often be expressing the \mathcal{P} function of some vertex-induced subgraph of a graph, it is convenient to adopt a shorthand notation. If the graph Γ , which we talk about is clear, and S is a subset of its set of vertices, then $\mathcal{P}(S)$ will be shorthand for $\mathcal{P}(\Gamma_S)$. Recall that Γ_S denotes the vertex-induced subgraph of the graph Γ , induced by the set of vertices S .

The other useful function is defined on bipartite graphs.

Definition 6 Let Γ be a bipartite graph with partitions V and W , where the set of vertices is equipped with a strict order. We define $\mathcal{B}_\Gamma(V, W)$ to be a vector of signs of length $2^{|W|}$, given by the following components

$$(\mathcal{B}_\Gamma(V, W))_k = SP(\#E(V \cup \text{Sel}(W, k)))$$

for $k = 1, \dots, 2^{|W|}$.

Again, if the graph Γ is clear from context, we will omit the subscript Γ , and simply write $\mathcal{B}(V, W)$ instead of $\mathcal{B}_\Gamma(V, W)$. These two functions can be explicitly defined on different representations of graphs, and these representations have potentially useful properties. We give these properties after we have given the theorem about the decomposition of the sign pattern matrices.

The row r can now be expressed (as its transpose, that is as a column) using \mathcal{B} and \mathcal{P} functions. As the goal is to represent a general column r (that is, any of the rows of any matrix B_i), we introduce these parameters for row r - its row index p , and its sign pattern matrix denoted by i . Therefore, $r_{p,i}$ is now expressed as:

$$r_{p,i} = \gamma_i c_{p,i}^1 c_p^2 \cdot (\mathcal{B}(\text{Sel}(O, p), \text{Aux}) \odot \mathcal{P}(\text{Aux}) \odot \mathcal{B}(\text{Sel}(I, i), \text{Aux})) \quad (7)$$

where I , Aux and O denote the sets of input, pure auxiliary and output vertices and \odot denotes the point-wise product. The order of the components corresponds to the order of factors in the entry-wise representation of r in 6.

In 7 γ_i is a scalar, corresponding to the factor $SP(\#E(B))$ in 6. So we can represent it using the \mathcal{P} function as

$$\gamma_i = (\mathcal{P}(I))_i$$

Also, $c_{p,i}^1$ is a constant scalar for every entry of a fixed row (hence depends on the row, and the choice of B_i), and corresponds to the expression $SP(\#E(B \leftrightarrow A))$ and it can be represented using the \mathcal{B} function

$$c_{p,i}^1 = (\mathcal{B}(\text{Sel}(I, i), O))_p$$

Finally, c_p^2 is a constant scalar for a fixed row, and does not depend on the choice of B_i , and corresponds to the term $SP(\#E(A))$. It can be represented using the function \mathcal{P}

$$c_p^2 = (\mathcal{P}(O))_p.$$

The three row-wise constant factors have been defined as components of vectors which depend on i or are constant. Then, by collecting the components across rows, and indexes i we can easily note the following deconstruction of the sign pattern matrices.

Theorem 2 Let $V = I \cup \text{Aux} \cup O$ be the set of vertices of the graph Γ , tri-partitioned into input, auxiliary and output vertices. Let

- $\gamma_i = (\mathcal{P}(\Gamma_I))_i$
- $\Delta_i = \text{diag}(\mathcal{B}(\text{Sel}(I, i), O))$
- $S = \text{diag}(\mathcal{P}(O))$
- $B = [\mathcal{B}(\text{Sel}(O, 1), \text{Aux}), \dots, \mathcal{B}(\text{Sel}(O, 2^{|O|}), \text{Aux})]^\tau$
- $N = \text{diag}(\mathcal{P}(\text{Aux}))$ and
- $\Omega_i = \text{diag}(\mathcal{B}(\text{Sel}(I, i), \text{Aux}))$

then

$$B_i = \gamma_i \Delta_i S B N \Omega_i.$$

Proof. The origin of γ_i is straightforward and the Δ_i and S matrices are a direct consequence of the \mathcal{P} and \mathcal{B} function representations of the scalars $c_{p,i}^1$ and c_p^2 given above.

The B matrix contains the first factor in the brackets in the expression 7 in each row, which is constant in i , but variable in row p .

Matrix N is the second factor in brackets in expression 7 spread across the diagonal of a diagonal matrix. That factor was constant in p and i and by presenting it as a diagonal matrix which multiplies B from the right, we achieve the pointwise multiplication of each row of B with that factor. Analogous reasoning is used for the matrix Ω_i with the difference that it is variable in i . \square

Collecting the results of theorems 1 and 2 we get the following corollary:

Corollary 1 Using the notation of theorems 1 and 2 the matrix M can be represented with respect to columns as:

$$M e_i = \varepsilon_i \gamma_i \Delta_i S B N \Omega_i \vec{\phi}.$$

While Theorem 2 completely decomposes the sign pattern matrices, for an actual calculation of the presented decomposition it is useful to have the explicit forms of the functions \mathcal{B} and \mathcal{P} . In the following section we present different representations of these functions, and present some of their properties which could be helpful in the application of the decomposition of Corollary 1.

6 Explicit representations of the \mathcal{P} and \mathcal{B} functions

The function \mathcal{B} has an elegant representation in terms of the adjacency matrix of the bipartite graph. If \mathcal{A} is the adjacency matrix of a bipartite graph, with partitions V and W , and all the labels of V precede the labels of W , then it is of the block form:

$$\mathcal{A} = \begin{bmatrix} 0 & C \\ C^\tau & 0 \end{bmatrix}$$

We now define the function $\hat{\mathcal{B}} : \{0, 1\}^n \rightarrow \{-1, 1\}^{2^n}$, such that

$$\hat{\mathcal{B}}(b_1, \dots, b_n) = \bigotimes_{i=1}^n \begin{bmatrix} 1 \\ SP(b_i) \end{bmatrix}. \quad (8)$$

It can be shown that if v is the modulo 2 sum of the columns of C , then

$$\mathcal{B}(V, W) = \hat{\mathcal{B}}(v).$$

That is, the \mathcal{B} function can be calculated directly from the adjacency matrix of the bipartite graph in question, by using the $\hat{\mathcal{B}}$ function. Moreover, the $\hat{\mathcal{B}}$ function is a monomorphism from the group $(\{0, 1\}^n, \oplus)$ to the group $(\{-1, 1\}^{2^n}, \odot)$, where \oplus and \odot represent modulo 2 addition and pointwise multiplication, respectively.

The $\hat{\mathcal{B}}$ representation of \mathcal{B} and the monomorphism property are important as described below. Given the adjacency matrix of the underlying graph we can efficiently compute a polynomial number of entries of the matrix-vector multiplication $B\vec{\phi}$ (Corollary 1), even though the mere length of a row of B is exponential in the number of auxiliary qubits. It will suffice to use the representation $\hat{\mathcal{B}}$ given on the right-hand side of 8, and $\vec{\phi}$ represented in the Kronecker product form, and use the following property of the scalar product on tensor spaces:

$$\left(\bigotimes_{i=1}^n X_i, \bigotimes_{i=1}^n Y_i\right) = \prod_{i=1}^n (X_i, Y_i),$$

when X_i and Y_i are of equal dimensions.

The monomorphism property also helps in the scenario where we want to calculate $B\Omega_i\vec{\phi}$. Since both the rows of B and the diagonal of Ω_i are represented by the \mathcal{B} functions, and hence by the $\hat{\mathcal{B}}$ functions, due to the monomorphism property, the pointwise product of a row in B and the diagonal of Ω_i is again representable in the $\hat{\mathcal{B}}$ form, which easily reads out of the adjacency matrix, so this becomes efficiently solvable as well.

However, there remains the problem of the matrix N , as what we really wish to calculate is $BN\Omega_i\vec{\phi}$, which is represented by the \mathcal{P} function. The \mathcal{P} function results the sign parities of the number of edges of all subgraphs of a given graph as a binary vector.

One way to explicitly represent it is by taking the positive part of the directed adjacency matrix of the given graph Γ . That is, we direct the graph in an arbitrary fashion, and in its directed adjacency matrix (which carries 1 and -1 depending on the direction of the directed edges, of the now directed graph) replace all -1 's with zeroes. If \mathcal{A} is that matrix then it can easily be seen that

$$(\mathcal{P}(\Gamma))_i = SP((\mathcal{A}[i]_2, [i]_2)),$$

where $[i]_2$ is the binary representation of $i - 1$ given as a vector.

If n is the number of vertices, this representation takes n^2 binary digits on input, as they make up the \mathcal{A} matrix.

An alternative representation uses $\binom{n}{2}$ binary digits in the form of an *edge binary list*, which we now define. Let E be an ordered set of pairs of vertices of Γ such that the label of the first vertex in a pair is strictly smaller than the label of the second, all in all $\binom{n}{2}$ of them, and let E be ordered lexicographically according to edges;

$$E = \{(v_i, v_j) | v_k \in V \text{ \& } i < j\}.$$

Then, for a given graph Γ , $V = V(\Gamma)$ with \mathcal{E} we denote the binary vector of length $\binom{n}{2}$ such that the i^{th} entry of \mathcal{E} is 1 if the i^{th} pair of vertices of E is adjacent in Γ and 0 otherwise. We call this vector the *edge binary list*. It is easy to see that the edge binary list uniquely characterises a simple graph. If Γ is a graph, and $\mathcal{E} = (b_1, \dots, b_{\binom{n}{2}})$ its *edge binary list* then $\mathcal{P}(\Gamma)$ can be explicitly given as

$$(\mathcal{P}(\Gamma))_i = \left(\mathcal{P} \left(b_1, \dots, b_{\binom{n}{2}} \right) \right)_i = \prod_{k=1}^{\binom{n}{2}} (-1)^{b_k X_1(i,k) X_2(i,k)},$$

where

$$X_1(i, k) = \left\lfloor \frac{i}{2^{f(k)}} \right\rfloor \mod 2,$$

and

$$X_2(i, k) = \left\lfloor \frac{i}{2^{(k - \binom{f(k)}{2} - 1)}} \right\rfloor \mod 2,$$

with

$$f(k) = \left\lfloor \frac{\sqrt{8k-7} + 1}{2} \right\rfloor.$$

The unappealing functions X_1 and X_2 can be explained more simply. Let (v_p, v_q) be the k^{th} entry of the set E . Then $X_1(i, k)$ is the q^{th} binary digit of binary represented $i - 1$, counting from the least significant digit. With the same notation $X_2(i, k)$ is the p^{th} binary digit of binary represented $i - 1$, counting from the least significant digit. This representation, even though seems to be the least elegant has one significant properties. For \mathcal{P} defined on edge binary lists,

$$\mathcal{P} : \{0, 1\}^{\binom{n}{2}} \rightarrow \{-1, 1\}^{2^n}$$

is a monomorphism from the group $(\{0, 1\}^{\binom{n}{2}}, \oplus)$ to the group $(\{-1, 1\}^{2^n}, \odot)$ where \oplus denotes pointwise modulo 2 addition, and \odot pointwise multiplication.

How to use this, or any other representation of the \mathcal{P} function to help efficiently evaluate or express $N\vec{\phi}$, or $BN\Omega_i\vec{\phi}$ in conjunction with the \mathcal{B} representation of \mathcal{B} remains an open question.

7 Discussion

We have presented a complete structural characterisation of the positive branch of a one-way pattern in terms of its matrix representation in the computational basis. This structure was shown to be intricate and complex yet admitting a high degree of regularity. While it remains unclear how to directly use this regularity to tackle problems such as direct simulation of unitaries in one-way model or full characterisation of pointless measurements and etc., however the proposed structure clearly emphasises the importance of the entanglement. Here, entanglement plays a crucial role in the mathematical structures which arise from mathematical descriptions of the process of quantum computation; If the pure auxiliary qubits are unconnected (unentangled), the matrix N , of the decomposition of Theorem 2, is the identity matrix. In that case, all the entries of the matrix realised by $R\Phi P$ can be quickly evaluated, once an open graph state and the measurement angles are given. If the pure auxiliary qubits are connected, this becomes an exponential task. We get a similar effect if we try to solve one restriction of the problem of simulating a given unitary. In this restricted problem an open graph state is given with the unitary, and it is promised that for a certain choice of angles, the positive branch will implement that unitary. For this promise problem it can be shown that it is easily and efficiently solvable if the pure auxiliary vertices of

the given graph are unconnected, for some families of graphs. Clearly, entanglement is again crucial. It is our belief that additional work on understanding the algebraic properties of the \mathcal{P} function, that is, of the graph states represented as sign patterns, may yield efficient algorithms for some instances of hard open problems in the one-way model. Such solved instances can benefit the understanding of quantum computation in general.

References

- [1] N. de Beaudrap, V. Danos, E. Kashefi & M. Roetteler (2008): *Quadratic Form Expansions for Unitaries*. In: *Theory of Quantum Computation, Communication, and Cryptography Third Workshop, TQC 2008 Tokyo, Japan*, number 5106 in Lecture Notes in Computer Science.
- [2] D. Browne, E. Kashefi, M. Mhalla & S. Perdrix (2007): *Generalized Flow and Determinism in Measurement-based Quantum Computation*. *New Journal of Physics* 9.
- [3] Vincent Danos & Elham Kashefi (2006): *Determinism in the one-way model*. *Phys. Rev. A* 74(5), p. 052310.
- [4] Niel deBeaudrap, Vincent Danos & Elham Kashefi (2006): *Phase map decomposition for unitaries*. (quant-ph/0603266), .
- [5] E. Kashefi, D. Markham, M. Mhalla & S. Perdrix (2009): *Information Flow in Secret Sharing Protocols*. EPTCS 9, p. 87.
- [6] R. Raussendorf & H.-J. Briegel (2001): *A one-way quantum computer*. *Physical Review Letters* 86(5188).
- [7] R. Raussendorf, D. E. Browne & H. J. Briegel (2003): *Measurement-based quantum computation with cluster states*. *Physical Review A* 68, p. 022312 [32 pages].
- [8] V. Danos, E. Kashefi & P. Panangaden (2007): *The Measurement Calculus*. *Journal of ACM* 54, p. 8 [45 pages].

8 Appendix

8.1 Summary of notation

Here we present a brief summary of the notation used throughout the paper. The algebra used is presented in the Dirac notation.

Qubit states A *qubit* is represented by a two-dimensional complex Hilbert space, called the qubit's state space. A *qubit state* is a vector of unit length in the qubit's state space. The *state space of an ensemble of qubits* is represented by the tensor product of the component state spaces, and the *state of an ensemble of qubits* is a vector of unit length in the state space of the ensemble. With $|0\rangle$ and $|1\rangle$ we denote unit orthonormal vectors in the state space of a qubit, and they constitute the *standard computational basis* of a qubit. $|\pm_\alpha\rangle$ denotes a vectors parameterised by the real angle α (and the choice of $+$ or $-$) defined with respect to the computational basis vectors as

$$|\pm_\alpha\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm e^{i\alpha}|1\rangle).$$

When $\alpha = 0$, we simply write $|\pm\rangle$.

Unitary transformations Z_α denotes a family of *phase shift unitary transformations*, parametrized by the real angle α , represented in the computational basis with the following matrix:

$$Z_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}.$$

When the Z_α rotation is applied to the i^{th} qubit of an ensemble of m qubits, the transformation of the state space of the ensemble is denoted with $\mathbf{Z}_\alpha^{(i)}$, which can be given explicitly with

$$\mathbf{Z}_\alpha^{(i)} = I^{\otimes(i-1)} \otimes Z_\alpha \otimes I^{\otimes(m-i)}.$$

Here, I denotes the identity operator on a single qubit state space. $\wedge Z$ denotes a unitary transformation on the state space of two qubits. In the computational basis it is given by the following matrix:

$$\wedge Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Note that this operator cannot be represented as a tensor product of single qubit transformations. Hence, it can be used to create *entangled states*, which are multi-qubit states which cannot be represented as tensor products of single-qubit states.

When the $\wedge Z$ transformation is applied to the component state subspace of the i^{th} and j^{th} qubit of an ensemble of m qubits, the transformation of the entire ensemble is denoted with $\wedge \mathbf{Z}_{i,j}$. The eigenvectors of the $\wedge \mathbf{Z}_{i,j}$ transformation are the vectors of the computational basis of the ensemble, with eigenvalue -1 if both the i^{th} and j^{th} qubit are in the state $|1\rangle$ and eigenvalue 1 otherwise.

Miscellaneous

- e denotes the basis of the natural logarithm.
- \mathbf{e}_i denotes the i^{th} vector of the canonical basis, i.e. a vector with entries 0 everywhere, except a 1 at the i^{th} entry.
- \otimes represents the tensor product. $X^{\otimes n}$ denotes the n -th tensor power of X , explicitly

$$X^{\otimes n} = \overbrace{X \otimes \cdots \otimes X}^{n \text{ times}}.$$

The tensor product of matrices (and also numerical vectors, as they are isomorphic to single row or column matrices) is called the Kronecker and defined explicitly as follows:

If A is an m -by- n matrix and B is a p -by- q matrix, then the Kronecker product $A \otimes B$ is the block matrix

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

- $SP(n)$, for an integer n denotes the *sign parity* function defined as

$$SP(n) = (-1)^n.$$

- X^τ denotes the transpose of the matrix (or vector) X .
- (\cdot, \cdot) denotes the symmetric dot product; If $X = [x_1, \dots, x_n]^\tau$ and $Y = [y_1, \dots, y_n]^\tau$ are vectors, then

$$(X, Y) = \sum_{i=1}^n x_i y_i.$$

- If Γ is a graph, and $A \subseteq V(\Gamma)$ a subset of the vertices of Γ , Γ_A denotes the vertex-induced subgraph of the graph Γ induced by the set of vertices A .
- If Γ is a graph $\#E(\Gamma)$ is the number of its vertices, i.e. $\#E(\Gamma) = |E(\Gamma)|$. If Γ_A is a subgraph of Γ , the graph designation can be dropped and $\#E(A)$ denotes $\#E(\Gamma_A)$. If A and B are disjoint subsets of the vertices of the graph Γ $\#E(A \leftrightarrow B)$ denotes the number of edges connecting the vertices in A to vertices in B in the graph Γ .
- \oplus denotes the modulo 2 addition. If $X = [x_1, \dots, x_n]^\tau$ and $Y = [y_1, \dots, y_n]^\tau$ are vectors of integers, then

$$X \oplus Y = [x_1 \oplus y_1, \dots, x_n \oplus y_n]^\tau.$$

- \odot denotes the pointwise vector product; If $X = [x_1, \dots, x_n]^\tau$ and $Y = [y_1, \dots, y_n]^\tau$ are vectors, then

$$X \odot Y = [x_1 \odot y_1, \dots, x_n \odot y_n]^\tau.$$

8.2 Proof of Theorem 1

Let $R\Phi P$ be the phase map decomposition [4] of the positive branch of a one-way pattern over m qubits, n of which are input, n output, and $a = m - 2n$ are pure auxiliary qubits. Also let $|i\rangle$ be a vector of the standard computational basis. Then we can directly derive the following:

$$\begin{aligned} R\Phi P|i\rangle &= I_{2^n} R\Phi P|i\rangle \\ &= \sum_{j=1}^{2^n} |j\rangle \langle j| R\Phi P|i\rangle \\ &= \sum_{j=1}^{2^n} |j\rangle \langle j| R\Phi(|i\rangle \otimes |+\rangle^{\otimes m-n}) \\ &= \sum_{j=1}^{2^n} |j\rangle \langle j| R\Phi_2 \Phi_1(|i\rangle \otimes |+\rangle^{\otimes m-n}) \\ &= \left(\left(\bigotimes_{k=1}^n \langle +\alpha_k | \right) |i\rangle \right) \sum_{j=1}^{2^n} |j\rangle \langle j| R\Phi_2(|i\rangle \otimes \left(\bigotimes_{k=n+1}^{m-n} |+\alpha_k\rangle \right) \otimes |+\rangle^{\otimes n}) \end{aligned}$$

For clarity reasons we temporarily omit the row-constant scalar $\left(\left(\bigotimes_{k=1}^n \langle +\alpha_k | \right) |i\rangle \right)$

$$\begin{aligned} &= \sum_{j=1}^{2^n} |j\rangle \langle j| R\Phi_2(|i\rangle \otimes \left(\bigotimes_{k=n+1}^{m-n} |+\alpha_k\rangle \right) \otimes |+\rangle^{\otimes n}) \\ &= \sum_{j=1}^{2^n} |j\rangle \langle j| \langle +|^{\otimes(m-n)} \otimes I_{2^n} \Phi_2(|i\rangle \otimes \left(\bigotimes_{k=n+1}^{m-n} |+\alpha_k\rangle \right) \otimes |+\rangle^{\otimes n}) \\ &= \sum_{j=1}^{2^n} |j\rangle \left(\langle +|^{\otimes(m-n)} \otimes \langle j| \right) \Phi_2(|i\rangle \otimes \left(\bigotimes_{k=n+1}^{m-n} |+\alpha_k\rangle \right) \otimes |+\rangle^{\otimes n}) \end{aligned}$$

We note that $\Phi_2 = \sum_{l=1}^{2^m} b_l |l\rangle \langle l|$ where b_l is the l^{th} diagonal element of the diagonal matrix Φ_2 ,

$$\begin{aligned}
&= \sum_{j=1}^{2^n} |j\rangle \left(\left(\langle + |^{\otimes(m-n)} \otimes \langle j | \right) \sum_{l=1}^{2^m} b_l |l\rangle \langle l| \right) (|i\rangle \otimes (\otimes_{k=n+1}^{m-n} |+\alpha_k\rangle) \otimes |+\rangle^{\otimes n}) \\
&= \sum_{j=1}^{2^n} |j\rangle \left(\sum_{l=1}^{2^{(m-n)}} b_{[(l-1)2^n+j]} \langle l | \langle j | \right) (|i\rangle \otimes (\otimes_{k=n+1}^{m-n} |+\alpha_k\rangle) \otimes |+\rangle^{\otimes n}) \tag{9}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{j=1}^{2^n} |j\rangle \left(\sum_{l=1}^{2^{(m-n)}} b_{[(l-1)2^n+j]} \langle l | \langle j | (|i\rangle \otimes (\otimes_{k=n+1}^{m-n} |+\alpha_k\rangle) \otimes |+\rangle^{\otimes n}) \right) \\
&= \sum_{j=1}^{2^n} |j\rangle \left(\sum_{l=1}^{2^{(m-n)}} b_{[(l-1)2^n+j]} \langle l | (|i\rangle \otimes (\otimes_{k=n+1}^{m-n} |+\alpha_k\rangle)) \right) \tag{10} \\
&= \sum_{j=1}^{2^n} |j\rangle \left(\sum_{l=1}^{2^{(m-2n)}} b_{[(i-1)2^{(m-n)}+(l-1)2^n+j]} \langle l | (\otimes_{k=n+1}^{m-n} |+\alpha_k\rangle) \right) \\
&= \sum_{j=1}^{2^n} \sum_{l=1}^{2^{(m-2n)}} b_{[(i-1)2^{(m-n)}+(l-1)2^n+j]} |j\rangle \langle l | (\otimes_{k=n+1}^{m-n} |+\alpha_k\rangle)
\end{aligned}$$

So now we summarise the entire expression (reintroducing the omitted scalar):

$$R\Phi P|i\rangle = \left(\left(\bigotimes_{k=1}^n \langle +\alpha_k | \right) |i\rangle \right) \sum_{j=1}^{2^n} \sum_{l=1}^{2^{(m-2n)}} b_{[(i-1)2^{(m-n)}+(l-1)2^n+j]} |j\rangle \langle l | \left(\bigotimes_{k=n+1}^{m-n} |+\alpha_k\rangle \right).$$

For simplicity, in (8) we omitted a global scaling factor of $2^{-(\frac{m-n}{2})}$, brought about by the scalar products $\langle + |^{\otimes(m-n)} \langle j | \langle l |$ where they are non-zero, and in (9) the global scaling factor $2^{-(\frac{n}{2})}$, caused by the product $\langle j | + \rangle^{\otimes n}$. The overall (omitted) scaling factor is $2^{-\frac{m}{2}}$.

The expression $((\otimes_{k=1}^n \langle +\alpha_k |) |i\rangle)$ is a scalar which depends on the column i , and we denote it by ε_i , also let

$$B_i = \sum_{j=1}^{2^n} \sum_{l=1}^{2^{(m-2n)}} b_{[(i-1)2^{(m-n)}+(l-1)2^n+j]} |j\rangle \langle l |$$

be a $2^n \times 2^{(m-2n)}$ matrix expressed in the computational basis that depends on the choice of column i with entries in $\{-1, 1\}$. Finally, denote the numeric representation in the computational basis of the vector $(\otimes_{k=n+1}^{m-n} |+\alpha_k\rangle)$ with $\vec{\phi}$, which is independ of the choice of the column. It corresponds to the quantum state of the auxiliary qubits after the local Z_α rotations, but before the entanglement procedure. The entire expression can then be rewritten in matrix notation as:

$$M\mathbf{e}_i = \varepsilon_i B_i \vec{\phi},$$

where \mathbf{e}_i is the i^{th} vector of the canonical basis. \square